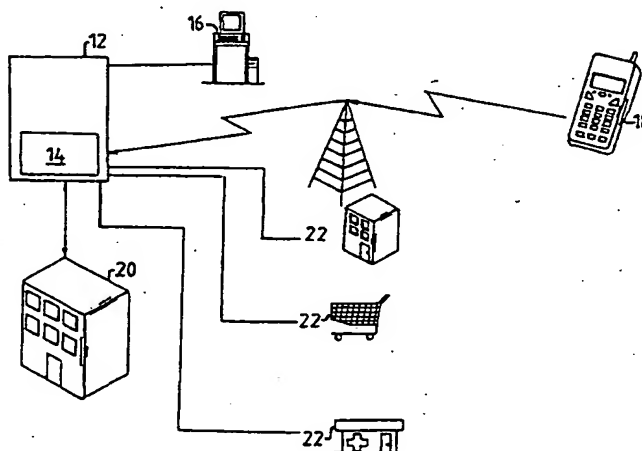




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : G07F 7/10 // 19:00	A1	(11) International Publication Number: WO 00/31699 (43) International Publication Date: 2 June 2000 (02.06.00)
(21) International Application Number: PCT/IB99/01844 (22) International Filing Date: 19 November 1999 (19.11.99) (30) Priority Data: 98/6510 22 November 1998 (22.11.98) ZA (71) Applicant (for all designated States except US): EASY CHARGE CELLULAR (PTY) LIMITED [ZA/ZA]; Grayston Ridge Office Park, Block B, 144 Katherine Street, 2146 Sandton (ZA). (72) Inventors; and (75) Inventors/Applicants (for US only): LIPTON, David, Ian [ZA/ZA]; 24 Hydewoods, Townshend Road, Hyde Park, 2196 Johannesburg (ZA). GRIFFIN, Michael, John [ZA/ZA]; 14 Molohe Street, Randpark Ridge, Randburg, 2194 Johannesburg (ZA). (74) Agent: LE ROUX, Marius; D.M. Kisch Inc., P.O. Box 781218, 2146 Sandton (ZA).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i>

(54) Title: METHOD OF, AND APPARATUS FOR, CONDUCTING ELECTRONIC TRANSACTIONS



(57) Abstract

This invention provides a method of conducting electronic transactions comprising the steps of: storing an encryption key in a memory means of a mobile telephone; selecting a financial transaction with the mobile telephone from a number of available financial transactions; providing transaction information; generating a transaction message from the selected financial transaction and transaction information; encrypting at least part of the transaction message; and transmitting the transaction message from the mobile telephone, over a wireless network. The invention extends to a mobile telephone having input means for inputting transaction information and for selecting a financial transaction from a number of available financial transactions; memory means for storing at least an encryption key; generating means for generating an at least partially encrypted transaction message from the transaction information, information relating to the selected financial transaction and the encryption key; and transmission means for transmitting the message over a wireless network.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

METHOD OF, AND APPARATUS FOR, CONDUCTING ELECTRONIC TRANSACTIONS

Technical Field

5 This invention relates to a method of, and apparatus for, conducting electronic transactions and more particularly, but not exclusively, to a method of and apparatus for conducting secure electronic transactions over a telephone network, such as a cellular telephone network.

10 Background Art

The use of telephones to conduct electronic financial transactions is well known in the art. Most commonly, Dual-Tone Multi-Frequency (DTMF) communication protocols of telephones are used to provide customers with access to banking services. This type of facility is only available to customers of a particular financial institution. Thus, only a
15 closed system is available and customers have to link third party accounts to their financial institutions to, for example, transfer funds to third party accounts.

The linking of third party accounts provides security in that customers do not have to manually enter third party account numbers every time a third party account is paid.
20 Incorrect entry of account numbers is avoided by linking third party accounts to a customer's financial institution. This linking process is cumbersome and limiting for customers and financial institutions and only linked accounts can be paid by customers.

25 Telephonic banking further provides for the purchase of goods or services by quoting a credit card number. In this case the credit card is not physically available to a merchant to read the card magnetically or to make a manual print or copy and this creates a difficulty from a security and authorisation perspective. With credit card transactions, the customer's financial institution pays the merchant or third party and accepts at least

partial liability in the case that the customer does not pay their credit card account. This type of transaction is also commonly used to purchase goods on the Internet. Pre-paid cellular airtime can also be purchased over a cellular telephone by providing a credit card number. Goods and services purchased are limited to those provided by a cellular service provider or those available on the Internet and, as stated above, a difficulty arises in that the financial institution incurs liability for payment.

Automatic Teller Machines (ATM's) provide a means for secure electronic banking. At an ATM, a card reader reads a bank card and a secret Personal Identification Number (PIN) is provided by a customer to authorise the transaction. Transaction messages are sent to switches or directly to banks or other financial institutions. These transaction messages are encrypted at a security level that is acceptable to financial institutions. ATMs are not readily accessible and are installed in fixed locations. Customers are also restricted at an ATM in that they cannot pay accounts which are not linked to their banking profile.

Objective of the Invention

It is an object of this invention to provide a method of, and apparatus for, conducting electronic transactions which, at least partially, alleviates some of the abovementioned difficulties.

Disclosure of the Invention

In accordance with this invention there is provided a method of conducting electronic transactions comprising the steps of:

- 25 storing an encryption key in a memory means of a mobile telephone;
- selecting a financial transaction with the mobile telephone from a number of available financial transactions;
- providing transaction information;
- generating a transaction message from the selected financial transaction and transaction
- 30 information;

encrypting at least part of the transaction message;
transmitting the transaction message from the mobile telephone, over a wireless network.

5 A further feature of the invention provides for the transaction message to be transmitted from the mobile telephone to a receiving station such as a bank or a switch.

A still further feature of the invention provides for the mobile telephone to be a cellular telephone or a satellite telephone.

10 There is also provided for the transaction information to include at least one bank account number or bank card number and an associated PIN.

15 Further features of the invention provide for the transaction message to include information relating to the selected transaction, a bank account number or bank card number and the PIN; for at least the PIN to be encrypted; and for the transaction message to include error check information to facilitate the authentication of the mobile telephone or SIM card at the receiving station and to facilitate the validation of the integrity of the message at the receiving station.

20 There is still further provided for the memory means to be a SIM card or to be an Integrated Circuit (IC) memory chip or a microprocessor.

25 Further features of the invention provide for an encryption algorithm to be stored on the memory means; and for copies of the encryption algorithm and the encryption key to be stored at the switch or the financial institution.

The invention extends to a mobile telephone having input means for inputting transaction information and for selecting a financial transaction from a number of available financial transactions;
30 memory means for storing at least an encryption key;

generating means for generating an at least partially encrypted transaction message from the transaction information, information relating to the selected financial transaction and the encryption key; and
transmission means for transmitting the message over a wireless network.

5

There is provided for the memory means to be a SIM card; alternatively, for the memory means to be an Integrated Circuit (IC) memory chip or a microprocessor.

10

There is provided for at least some of the transaction information, such as a bank account number or a bank card number, to be stored on the memory means.

There is provided for an encryption algorithm to be stored in the memory means and for the encryption algorithm to generate a new encryption key for each new encryption message generated.

15

A further feature of the invention provides for error check information to be transmitted with the message. The error check information facilitates the validation of the integrity of a transaction message received by a receiving station and also facilitates the authentication of the mobile phone or SIM card from which the message is received at the
20 receiving station.

Further features of the invention provide for the receiving station to be a switch or a financial institution; and

25

for the financial institution or switch to effect a financial transaction in response to receiving the message.

These and other features of the invention are described in more detail below.

Brief Description of the Drawing

A preferred method and embodiment of the invention is described below by way of example only, and with reference to the accompanying drawing, which shows a schematic block diagram of a method of and apparatus for conducting electronic transactions.

Best Mode of Carrying out the Invention

With reference to the accompanying drawing, a method for conducting an electronic transaction is shown schematically, and apparatus for use in the method are generally indicated by reference numeral 10.

The method utilises and includes the following apparatus: a switch 12 which houses a secure translator 14, a point of sale (POS) terminal 16, a mobile telephone such as a cellular telephone 18, a financial institution 20 and at least one content provider 22.

The switch 12 is connected to at least one cellular telephone 18 via a cellular telephone network and is further connected by means of a fixed land-based communication line to at least one financial institution 20 and at least one POS terminal 16.

The content providers 22 subscribe to the services of the switch 12, which provides a user of a cellular telephone 18 with the means to conduct a secure electronic transaction between a content provider 22 and a financial institution 20. The switch 12 has the facility to receive transaction messages transmitted over a cellular telephone network by a cellular telephone 18 and forward the messages to a financial institution 20 with the instructions necessary to effect a transaction involving a particular content provider 22 in accordance with the transaction message. Furthermore, a transaction message received by the switch 12 contains encrypted information which is translated, by the translator 14, into an encryption format that the financial institution 20 will have the means to interpret.

A SIM card of the cellular telephone 18 has an initial encryption key and an encryption algorithm stored thereon as described below. A unique initial encryption key is generated by the switch 12 to be associated with a specific SIM card during the manufacture of the SIM cards. Transportation of a database of initial encryption keys to a manufacturer of the SIM cards takes place in at least two distinct separate paths. Each initial encryption key is divided into at least two parts so that each part of an initial encryption key is rendered useless by itself. These divided parts are then transported via the two paths so that the transportation from the switch to the manufacturer of the initial encryption keys is secure. The initial encryption keys are reassembled on arrival at the manufacturer of the SIM cards where a particular initial encryption key is stored on a secure zone of a particular SIM card during the manufacturing process. A database of initial encryption keys and corresponding SIM identities is stored securely within translator 14 resident at the switch 12.

In addition to the installation of the initial encryption key on a SIM card an encryption algorithm is also stored on the SIM cards. The encryption algorithm is used to encrypt transaction messages with the use of encryption keys. Transaction messages are transmitted from the cellular telephone 18 and consist of a bank account number or bank card number and an associated PIN (referred to in this specification as the "transaction information") and information relating to a selected transaction from a number of available choices. A menu of available choices may be displayed on a screen of the cellular telephone 18 or may be made available in any convenient manner such as in printed format. The transaction message is generated by a generating means in the mobile telephone. The generating means can be software stored in the memory means or can be dedicated hardware for generating transaction messages or a combination of both.

Once a customer has purchased a SIM card for use in a cellular telephone, a registration process is required in order to initialize a secure transaction facility. The registration process involves storing a user's banking details such as the user's bank account or bank card number on a secure zone of the SIM card. It is envisaged that this will take place at

the POS terminal 16. Customers swipe the bank card through a magnetic strip reader at the POS terminal 16 thereby enabling the POS terminal 16 to access their banking details. The POS terminal 16 then stores the banking details in a secure zone on the SIM card. A request for the registration of this particular SIM card identity within the system is transmitted to the switch 12 from the POS terminal 16. It will be appreciated that the banking details of a user can be transmitted for storage on the SIM card over a cellular network or can be stored on the SIM card by inserting the SIM card into a writer at the POS terminal 16.

- 10 On receipt of the registration request message, the switch 12 validates the integrity of the information received using error check information that authenticates the POS terminal 16 and SIM card before returning a response message that is encrypted using the same initial encryption key. The error check information is transmitted with all messages that are transmitted in the system. The error check information allows for checking of both the validity of the source of a message and the correctness of a received message.

- The SIM card now validates the accuracy of the response message from the switch 12. Both the switch 12 and SIM card, using information from both the request and response messages, update the initial encryption key using the encryption algorithm for use in the next transaction. Using an algorithm common to the SIM card and the switch, a new encryption key is derived for each new message in the system. An encryption technique such as this will ensure a different encryption key for each transaction message of each individual cellular telephone.

- 25 After registration, the cellular telephone provides a user interface that enables the user to select from a menu of financial transactions. This functionality, i.e. the structure and content of the menu, is provided in the cellular telephone firmware, using a SIM toolkit, a Wireless Application Protocol (WAP) interface or a means provided in another format such as printed hardcopy format as described above. A hardcopy menu will have numbers corresponding to available financial transactions for keying the numbers into the

input means or keypad of the mobile telephone. It will be appreciated that the input means can be electronic input means as opposed to being a keypad.

5 The user is prompted to select a transaction as well as a bank account or card from their banking profiles. As with transactions initiated at an Automatic Teller Machine (ATM) terminal, a bank Personal Identification Number (PIN) is requested from user to authorise the transaction. Once the transaction information has been obtained from the user, a transaction message is generated and transmitted via a cellular network to the switch 12. The transaction message comprises an encrypted bank PIN, which is a product of the
10 newly generated encryption key, information relating to the selected transaction as well as transaction information together with error check information.

In this embodiment, the transport mechanism for the transaction message is a Short Message Service (SMS). On receiving the transaction message the switch 12 validates
15 the accuracy of the transaction message by utilising the error check information and relays the instruction to the appropriate content provider 22 and/or financial institution 20. Information of a financial settlement is forward to a financial institution 20 after translation thereof by the translator 14 to an encrypted message with an encryption key that it has in common with the financial institution. All transaction messages are sent and
20 forwarded together with error check information to ensure successful and accurate transmission and receipt.

The method of conducting electronic transactions described herein is a secure method in that at least part of the information transmitted from the mobile telephone 18 is encrypted
25 and cannot be read if it is fraudulently intercepted. The translator used at the switch 12 is secure in that the translation process cannot be accessed or read and the translator itself cannot be opened to access the information therein. A translator as is known in the art is used. Such a translator will erase all information if it is tampered with and no electronic access to the translation process from outside such a translator is possible.

The information transmitted from the switch to a financial institution or to a content provider is also encrypted and can not be understood if intercepted.

5 The transaction method is secure and customers using a mobile telephone can pay any third party accounts from their mobile telephones. Third party accounts do not have to be linked to a customer's banking profile to transfer funds to these accounts. Third parties subscribe to the services of the switch 12 and do not have to be linked to a financial institution.

10 The invention is not limited to the precise details as described herein. For example, instead of the switch 12 being in fixed land-based communication with a financial institution 20 or content provider 22, the switch 12 can be in wireless communication with a financial institution 20 or content provider 22. Also, the memory means can be an integrated circuit memory chip or a microprocessor having embedded memory instead of
15 being a SIM card. The mobile phone used can be a cell phone as is known in the art or can be a satellite telephone any other portable device capable of accessing a wireless communication network. It is also unnecessary to store bank account numbers or bank card numbers on the memory means of the mobile telephone. These may be manually entered using the input means of a mobile terminal or keypad of a mobile telephone.

CLAIMS

- 5 1. A method of conducting electronic transactions comprising the steps of: storing an encryption key in a memory means of a mobile telephone; selecting a financial transaction with the mobile telephone from a number of available financial transactions; providing transaction information; generating a transaction message from the selected financial transaction and transaction information; encrypting at least part of the transaction message; transmitting the transaction message from the mobile telephone, over a wireless network.
- 10 2. A method as claimed in claim 1 in which the transaction message is transmitted from the mobile telephone to a receiving station.
- 15 3. A method as claimed in claim 2 in which the receiving station is a bank.
4. A method as claimed in claim 2 in which the receiving station is a switch.
- 20 5. A method as claimed in any one of the preceding claims in which the mobile telephone is a cellular telephone or a satellite telephone.
6. A method as claimed in any one of the preceding claims in which the transaction information includes at least a PIN.
- 25 7. A method as claimed in claim any one of claims 1 to 5 in which the transaction information includes at least one bank account number or bank card number.
8. A method as claimed in claim 7 wherein the bank card number or the bank account number is stored in the memory means.

9. A method as claimed in any one of the preceding claims in which the transaction message includes information relating to the selected transaction, a bank account number and a PIN.
- 5 10. A method as claimed in any one of claims 1 to 7 in which the transaction message includes information relating to the selected transaction, a bank card number and a PIN.
- 10 11. A method as claimed in claim 8 or 9 in which at least the PIN is encrypted before transmission of the transaction message.
- 15 12. A method as claimed in any one of the preceding claims in which the transaction message includes error check information to facilitate the validation of the integrity of the transmitted message and to facilitate the authentication of the source from which the message is transmitted.
- 20 13. A method as claimed in any one of the preceding claims in which the memory means is a SIM card.
- 25 14. A method as claimed in any one of claims 1 to 12 in which the memory means is an Integrated Circuit (IC) memory chip.
- 30 15. A method as claimed in any one of claims 1 to 12 in which the memory means is a microprocessor.
16. A method as claimed in any one of the preceding claims in which an encryption algorithm is stored on the memory means.
17. A method as claimed in claim 16 in which copies of the encryption algorithm and the encryption key are stored at the switch.

18. A method as claimed in claim 16 in which copies of the encryption algorithm and the encryption key are stored at the financial institution.

5 19. A mobile telephone having input means for inputting transaction information and for selecting a financial transaction from a number of available financial transactions; memory means for storing at least an encryption key; generating means for generating an at least partially encrypted transaction message from the transaction information, information relating to the selected financial transaction and the encryption key; and
10 transmission means for transmitting the message over a wireless network.

20. A mobile telephone as claimed in claim 19 in which the memory means is a SIM card.

15 21. A mobile telephone as claimed in claim 19 in which the memory means is an Integrated Circuit (IC) memory chip.

22. A mobile telephone as claimed in claim 19 in which the memory means is a microprocessor.

20 23. A mobile telephone as claimed in any one of claim 19 to 22 in which an encryption algorithm is stored in the memory means.

25 24. A mobile telephone as claimed in claim 23 in which the encryption algorithm generates a new encryption key for each new financial transaction selected and subsequent transaction message generated.

30 25. A mobile telephone as claimed in any one of claim 19 to 23 in which error check information is transmitted with the transaction message.

26. A mobile telephone as claimed in claim 25 in which the error check information facilitates the authentication of the mobile telephone or SIM card and facilitates the validation of the integrity of the transaction message.

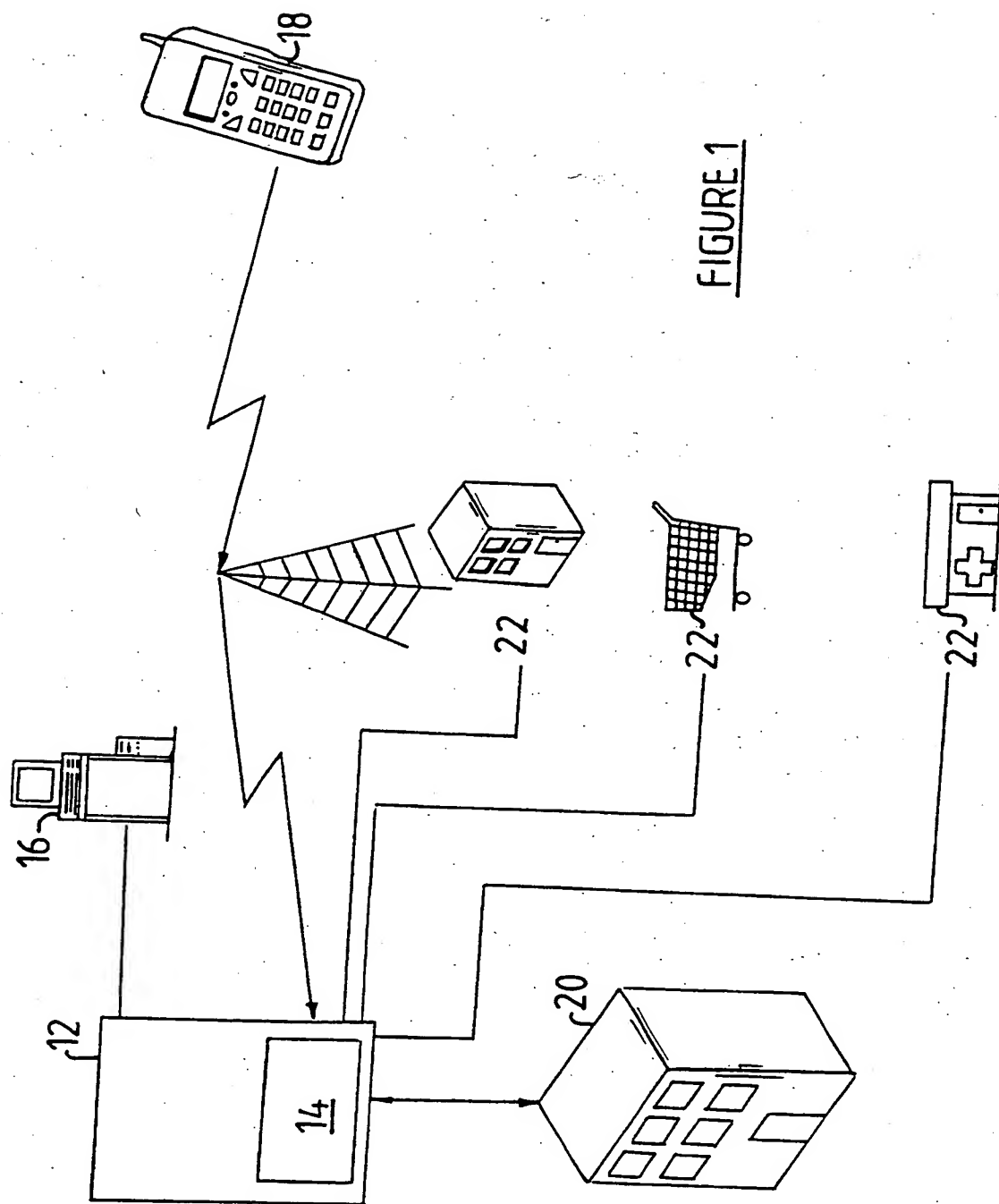
5 27. A mobile telephone as claimed in any one of claims 19 to 26 wherein the mobile phone transmits a transaction message to a receiving station.

28. A mobile phone as claimed in any one of claims 18 to 26 wherein the mobile telephone transmits a transaction message to a financial institution.

10

29. A mobile telephone as claimed in claim 27 in which the telephone transmits a transaction message to a switch or to a financial institution acting as a receiving station.

15 30. A mobile telephone as claimed in claim 19 in which transaction information including a bank account number or bank card number but excluding a PIN is stored in the memory means.



INTERNATIONAL SEARCH REPORT

Int. Patent Application No.

PCT/IB 99/01844

A. CLASSIFICATION OF SUBJECT MATTER

IPC-7 G07F7/10 //G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98 52151 A (ACCESS SECURITY SWEDEN AB ;SJOEBLOM HANS (SE)) 19 November 1998 (1998-11-19)	1-3,5,7, 8,14,16, 19,21, 23,27-30
A	page 2, line 9 -page 14, line 19 figure 5	3,4,6,9, 10
Y	WO 98 34203 A (QUALCOMM INC) 6 August 1998 (1998-08-06)	1-3,5,7, 8,14,16, 19,21, 23,27-30
A	page 3, paragraph 3 -page 4, paragraph 1 page 6, paragraph 1 -page 11, paragraph 1 claims; figures 1,3,4,7	6,9,11
	-/-	

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

10 February 2000

Date of mailing of the international search report

18/02/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Bocage, S

INTERNATIONAL SEARCH REPORT

Inte onal Application No

PCT/IB 99/01844

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>W0 98 47116 A (ERICSSON TELEFON AB L M) 22 October 1998 (1998-10-22)</p> <p>page 7, line 1 -page 11, line 26 page 26, line 13 -page 29, line 21 figures 1,5A,5B</p>	<p>1-3,5-8, 13,14, 16, 19-21, 23,27,28</p>
A	<p>W0 97 45814 A (VAZVAN BEHRUZ) 4 December 1997 (1997-12-04)</p>	

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/IB 99/01844

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9852151 A	19-11-1998	AU 7560298 A SE 9701814 A	08-12-1998 16-11-1998
WO 9834203 A	06-08-1998	AU 5963898 A	25-08-1998
WO 9847116 A	22-10-1998	AU 7094398 A EP 0976116 A	11-11-1998 02-02-2000
WO 9745814 A	04-12-1997	FI 962553 A FI 971248 A FI 970767 A EP 0960402 A FI 971009 A	25-11-1997 26-04-1997 20-10-1997 01-12-1997 26-04-1997

THIS PAGE BLANK (USPTO)